

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019110

International filing date: 21 December 2004 (21.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-433904
Filing date: 26 December 2003 (26.12.2003)

Date of receipt at the International Bureau: 17 February 2005 (17.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

24.12.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 2 月 2 6 日
Date of Application:

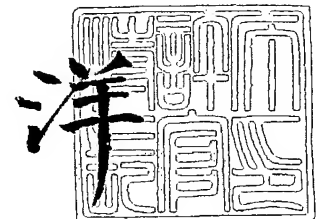
出 願 番 号 特 願 2 0 0 3 - 4 3 3 9 0 4
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 4 3 3 9 0 4]

出 願 人 松 下 電 器 産 業 株 式 有 限 公 司
Applicant(s):

2 0 0 5 年 2 月 4 日

特 許 庁 長 官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 2048150095
【提出日】 平成15年12月26日
【あて先】 特許庁長官 殿
【国際特許分類】 G09C 5/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 布田 裕一
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 大森 基司
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100090446
 【弁理士】
 【氏名又は名称】 中島 司朗
【手数料の表示】
 【予納台帳番号】 014823
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9003742

【書類名】特許請求の範囲**【請求項 1】**

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムであって

、
前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、

前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備えること

を特徴とする鍵発行システム。

【請求項 2】

鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムであって、

前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、

前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、

前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備えること

を特徴とする鍵発行システム。

【請求項 3】

前記証明書発行サーバは、さらに、前記公開鍵が前記発行識別子に基づいた前記素数を用いて生成されているかを判定する鍵判定部を備えること

を特徴とする請求項 2 記載の鍵発行システム。

【請求項 4】

前記素数生成部は、前記発行識別子情報に基づいて 2 つの素数を生成すること

を特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載の鍵発行システム。

【請求項 5】

前記素数生成部は、前記発行識別子情報 $ID I$ 及び $0 \leq c_1, c_2 < ID I$ を満たす予め与えられた整数 c_1, c_2 に対して、 $N_1 = c_1 \bmod ID I$ 及び $N_2 = c_2 \bmod ID I$ を満たす素数 N_1 及び N_2 を生成すること

を特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載の鍵発行システム。

【請求項 6】

前記鍵判定部は、前記素数 N_1 及び N_2 の積である前記公開鍵 $n (= N_1 \times N_2)$ と前記整数 c_1, c_2 に対して、 $n - c_1 \times c_2$ が発行識別子情報 $ID I$ で割り切れることを判定すること

を特徴とする請求項 5 記載の鍵発行システム。

【請求項 7】

前記素数生成部は、第 1 素数 q 、乱数 R 及び前記発行識別子情報 $ID I$ を用いて $N = 2 \times R \times ID I \times q + 1$ で表される素数 N を生成すること

を特徴とする請求項 1 から請求項 6 のいずれか 1 項に記載の鍵発行システム。

【請求項 8】

前記素数生成部は、 len ビットの素数を生成し、

$len_q \geq len / 2$ を満たす len_q ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 I D I、前記第 1 の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times I D I \times q + 1$ なる素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \pmod{N}$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 1 から請求項 7 のいずれか 1 項に記載の鍵発行システム（ここで、 a^x は a の x 乗を示す）。

【請求項 9】

前記素数生成部は、 len ビットの素数を生成し、

$lenq \geq len/2$ を満たす $lenq$ ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 I D I、前記第 1 の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times I D I \times q + 1$ なる素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 1 から請求項 7 のいずれか 1 項に記載の鍵発行システム（ここで、 $GCD(X, Y)$ は X と Y の最大公約数を示す）。

【請求項 10】

前記鍵判定部は、前記公開鍵 n に対して、 $n-1$ が前記発行識別子情報 I D I で割り切れることを判定すること

を特徴とする請求項 1 から請求項 9 のいずれか 1 項に記載の鍵発行システム。

【請求項 11】

前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むこと

を特徴とする請求項 1 から請求項 10 のいずれか 1 項に記載の鍵発行システム。

【請求項 12】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置であって、

前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、

前記秘密鍵は発行識別子情報に基づいて生成された複数の素数を含むこと

を特徴とする端末装置。

【請求項 13】

鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置であって、

前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、

前記秘密鍵は発行識別子情報に基づいて生成された複数の素数を含むこと

を特徴とする端末装置。

【請求項 14】

前記秘密鍵は前記発行識別子情報に基づいて生成された 2 つの素数を含むこと

を特徴とする請求項 12 または請求項 13 記載の端末装置。

【請求項 15】

前記 2 つの素数は、前記発行識別子情報 I D I 及び $0 \leq c_1$, $c_2 < I D I$ を満たす予

め与えられた整数 c_1 , c_2 に対して、 $N_1 = c_1 \bmod IDI$ 及び $N_2 = c_2 \bmod IDI$ を満たす素数 N_1 及び N_2 であること

を特徴とする請求項 12 から請求項 14 のいずれか 1 項に記載の端末装置。

【請求項 16】

前記複数の素数は、第 1 素数 q 、乱数 R 及び前記発行識別子情報 IDI を用いて $N = 2 \times R \times IDI \times q + 1$ で表されること

を特徴とする請求項 12 から請求項 14 のいずれか 1 項に記載の端末装置。

【請求項 17】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバであって、

前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備えること

を特徴とする鍵発行サーバ。

【請求項 18】

前記素数生成部は、前記発行識別子情報に基づいて 2 つの素数を生成すること

を特徴とする請求項 17 記載の鍵発行サーバ。

【請求項 19】

前記素数生成部は、前記発行識別子情報 IDI 及び $0 \leq c_1$, $c_2 < IDI$ を満たす予め与えられた整数 c_1 , c_2 に対して、 $N_1 = c_1 \bmod IDI$ 及び $N_2 = c_2 \bmod IDI$ を満たす素数 N_1 及び N_2 を生成すること

を特徴とする請求項 17 または請求項 18 記載の鍵発行システム。

【請求項 20】

前記素数生成部は、第 1 素数 q 、乱数 R 及び前記発行識別子情報 IDI を用いて $N = 2 \times R \times IDI \times q + 1$ で表される素数 N を生成すること

を特徴とする請求項 17 から請求項 19 のいずれか 1 項に記載の鍵発行サーバ。

【請求項 21】

前記素数生成部は、 len ビットの素数を生成し、

$len_q \geq len/2$ を満たす len_q ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 IDI 、前記第 1 の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times IDI \times q + 1$ なる素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \bmod N$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \bmod N$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 17 から請求項 20 のいずれか 1 項に記載の鍵発行サーバ。

【請求項 22】

前記素数生成部は、 len ビットの素数を生成し、

$len_q \geq len/2$ を満たす len_q ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 IDI 、前記第 1 の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times IDI \times q + 1$ なる素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \bmod N$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 17 から請求項 20 のいずれか 1 項に記載の鍵発行サーバ。

【請求項 23】

前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むことを特徴とする請求項 17 から請求項 22 のいずれか 1 項に記載の鍵発行サーバ。

【請求項 24】

素数を生成する素数生成装置であって、

前記素数生成装置は、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、を備えることを特徴とする素数生成装置。

【請求項 25】

前記素数生成部は、前記発行識別子情報 $ID I$ 及び $0 \leq c < ID I$ を満たす予め与えられた整数 c に対して、 $N = c \bmod ID I$ を満たす素数 N を生成することを特徴とする請求項 24 記載の素数生成装置。

【請求項 26】

前記素数生成部は、第 1 素数 q 、乱数 R 及び前記発行識別子情報 $ID I$ を用いて $N = 2 \times R \times ID I \times q + 1$ で表される素数 N を生成することを特徴とする請求項 24 または請求項 25 記載の素数生成装置。

【請求項 27】

前記素数生成部は、 len ビットの素数を生成し、

$len q \geq len / 2$ を満たす $len q$ ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 $ID I$ 、前記第 1 の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times ID I \times q + 1$ なる素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \bmod N$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \bmod N$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 24 から請求項 26 のいずれか 1 項に記載の素数生成装置。

【請求項 28】

前記素数生成部は、 len ビットの素数を生成し、

$len q \geq len / 2$ を満たす $len q$ ビットの第 1 の素数 q を生成する素数情報生成手段と、

乱数 R を生成する乱数生成手段と、

前記発行識別子情報 $ID I$ 、前記第 1 の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times ID I \times q + 1$ なる素数候補 N を生成する素数候補生成部と、

前記素数候補 N に対し、 $2^{(N-1)} = 1 \bmod N$ を満たすか否かを判定する第 1 の素数判定部と、

前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第 2 の素数判定部と、を備えること

を特徴とする請求項 24 から請求項 26 のいずれか 1 項に記載の素数生成装置。

【請求項 29】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから RSA 暗号の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行方法であって、

前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、

前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備えること

を特徴とする鍵発行方法。

【請求項 3 0】

鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行方法であって、

前記鍵発行サーバは、データを送信する送信部と、データを受信する受信部と、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、

前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、

前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備えること

を特徴とする鍵発行方法。

【請求項 3 1】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、

前記プログラムは、素数を含む前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵を格納する公開鍵格納ステップと、を前記端末装置に実行させ、

前記秘密鍵は発行識別子情報に基づいて生成された素数を含むこと
を特徴とするプログラム。

【請求項 3 2】

鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、

前記プログラムは、前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵証明書を格納する公開鍵証明書格納ステップと、を前記端末装置に実行させ、

前記秘密鍵は発行識別子情報に基づいて生成された素数を含むこと
を特徴とするプログラム。

【請求項 3 3】

鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバに実行させるプログラムであって、

前記プログラムは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成ステップと、を前記鍵発行サーバに実行させること

を特徴とするプログラム。

【請求項 3 4】

素数を生成する素数生成装置に実行させるプログラムであって、

前記プログラムは、発行識別子を生成する発行識別子生成ステップと、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、を前記素数生成装置に実行させること

を特徴とするプログラム。

【請求項 3 5】

請求項 3 1 から請求項 3 4 のいずれか 1 項に記載のプログラムを記録した媒体。

【書類名】明細書

【発明の名称】鍵発行システム、鍵発行装置、素数生成装置、鍵発行方法、素数生成方法及び記録媒体

【技術分野】

【0001】

本発明は、素因数分解を安全性の根拠として実現する暗号などの情報セキュリティ技術に関する。

【背景技術】

【0002】

近年、コンピュータ技術及び通信技術に基づくデータ通信が広く普及してきており、このデータ通信においては、秘密通信方式やデジタル署名方式が用いられる。ここで、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行う方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、発信者の身元を証明したりする通信方式である。

【0003】

1. 公開鍵暗号方式

これらの秘密通信方式又はデジタル署名方式においては、公開鍵暗号方式とよばれる暗号方式が用いられる。公開鍵暗号方式を用いる秘密通信では、暗号化鍵と復号化鍵とが異なり、復号化鍵は秘密にするが、暗号化鍵は公開する。秘密にする復号化鍵を秘密鍵と呼び、公開する暗号化鍵を公開鍵と呼ぶ。通信相手が多数のとき、共通鍵暗号では通信相手間で鍵をもつ必要があるが、公開鍵暗号では通信相手が一つの固有の鍵をもつだけで通信可能になるため、通信相手が増えても、共通鍵暗号より鍵の数が少なくてよい。このように、公開鍵暗号は多数の通信相手と通信を行うのに適しており、不可欠な基盤技術である。

【0004】

公開鍵暗号方式の1種であるRSA暗号方式では、整数の素因数分解問題を解くことが、計算量の上で困難であることを安全性の根拠としている。素因数分解問題とは、 p 、 q を素数とし、整数 $n = p \times q$ とすると、整数 n に対して、素数 p 、 q を求める問題である。ここで、 \times は通常の乗算である。一般に p 、 q が1024ビットの数のように大きい場合は、素因数分解問題が困難である。それにより、RSA暗号方式の公開鍵から秘密鍵を求めることや、秘密鍵を持たないユーザが暗号文から平文を求めることが、困難になる。なお、素因数分解問題については、非特許文献1の144～151ページに詳しく述べられている。

【0005】

(素因数分解問題を応用するRSA暗号方式)

素因数分解問題を応用するRSA暗号方式について説明する。

(1) 鍵の生成

次に示すようにして公開鍵及び秘密鍵を計算する。

- ・ ランダムに大きい素数 p 、 q を選択し、その積 $n = p \times q$ を計算する。

【0006】

- ・ $(p-1)$ 及び $(q-1)$ の最小公倍数 $L = \text{LCM}(p-1, q-1)$ を計算する。
- ・ L と互いに素で L より小さい自然数 e をランダムに選ぶ。

$$1 \leq e \leq L-1, \text{GCD}(e, L) = 1$$

ここで、 $\text{GCD}(e, L)$ は、 e と L の最大公約数を示している。

- ・ $e \times d = 1 \pmod{L}$ を満たす d を計算する。 $\text{GCD}(e, L) = 1$ より、このような d は必ず存在する。このようにして、得られた整数 e 及び整数 n が、公開鍵である。また、整数 d が、秘密鍵である。ここで、 $x \pmod{y}$ は、 x を y で割った余りを示す。

【0007】

(2) 暗号文の生成

公開鍵である整数 e 及び整数 n を用いて、平文 m に暗号演算を施して暗号文 c を計算する。

$$c = m^e \bmod n$$

なお、この明細書において、演算子 $^$ は、べき乗を示す。例えば、 A^x は、 $x > 0$ のときは A を x 回乗じたものを示す。

【0008】

(3) 復号文の生成

秘密鍵である整数 d を用いて、暗号文 c に復号演算を施して復号文 m' を計算する。

$$m' = c^d \bmod n$$

なお、

$$\begin{aligned} m' &= c^d \bmod n \\ &= (m^e)^d \bmod n \\ &= m^{(e \times d \bmod L)} \bmod n \\ &= m^1 \bmod n \\ &= m \bmod n \end{aligned}$$

であるので、復号文 m' は、平文 m と一致する。

【0009】

また、RSA暗号については、非特許文献2の110～113ページに詳しく説明されている。

上記に示した素因数分解を応用したRSA暗号における公開鍵の生成のステップにおいて、素数生成が行われる。素数生成については、非特許文献3の145～154ページに詳しく説明されている。素数生成方法には、確率的素数生成法と確定的素数生成方法がある。確率的素数生成法により生成される素数は、「素数である確率が高い」数であり、100%素数であるとは限らない。一方、確定的素数生成方法は、確実に素数である数を生成する。確率的素数生成方法及び確定的素数生成方法については、非特許文献2に詳しく説明されている。以下では、確定的素数生成方法について説明する。

【0010】

2. 従来例1-確定的素数生成方法

確定的に素数を生成することができるMaurer法による確定的素数生成方法について説明する。ここで、Maurer法については、非特許文献3の152～153ページに詳しく説明されている。

前記確定的素数生成方法では、次に示すステップを繰り返すことにより、素数を生成する。あらかじめビットサイズ len_q の素数 q が与えられている。

【0011】

(ステップ1) $(len_q - 1)$ ビットの乱数 R を選択する。なお、乱数 R の最上位ビットは、必ず1となるようにする。

(ステップ2) 数 N を以下の式により計算する。

$$N = 2 \times q \times R + 1$$

(ステップ3) 数 N が素数であるか否かを、次に示す第1判定及び第2判定がともに、成立する場合に、素数と判定する。他の場合に、素数でないと判定する。

【0012】

(第1判定) $2^{(N-1)} = 1 \bmod N$

(第2判定) $GCD(2^{(2R)} - 1, N) = 1$

素数であると判定される場合には、数 N を素数として出力する。素数でないと判定される場合には、ステップ1へ戻って、素数が出力されるまで、処理を繰り返す。

ステップ3で述べられている判定方法は、Pocklingtonの素数判定法とよばれ、非特許文献3の144ページに詳しく述べられている。Pocklingtonの素数判定法では、 $N = 2 \times q \times R + 1$ の q が素数であり、第1判定及び第2判定の結果が真であれば、必ず、 N が素数になる。そのため、確定的に素数であることを判定でき、確定的な素数生成が可能になる。

【0013】

このようにして、Maurer法による確定的素数生成方法では、サイズ $len q$ の素数 q を基にして、サイズ $2 \times len q$ の素数 N を生成する。従って、Maurer法による確定的素数生成方法を用いて所定長の素数を生成する場合には、前記所定長以下の素数の生成を繰り返し行う。例えば、512ビット長の素数を生成する場合には、あらかじめ与えられた8ビットの素数を基にして16ビットの素数を生成する。次に、生成した16ビットの素数を基にして32ビットの素数を生成する。次に、生成した32ビットの素数を基にして64ビットの素数を生成する。以下同様の素数生成を繰り返して、512ビットの素数を生成する。

【0014】

なお、前記第2判定を次の判定に代えてもよい。

$$(\text{第3判定}) \quad 2^{(2R)} \neq 1 \pmod{N}$$

上記第3判定方法は、非特許文献4に詳しく述べられている。以降、こちらの判定方法を使用していく。

3. 複数の鍵発行サーバをもつ鍵発行システム

公開鍵暗号の鍵発行システムでは、ユーザが鍵を生成する場合や、鍵発行サーバによりユーザに鍵を発行する場合がある。鍵発行サーバにより鍵を発行する場合、ユーザに鍵を発行するサーバは一台であることが多い。しかし、ユーザが増加すると、上記のような素数生成方法は、複数回べき乗を行うことにより計算量が大きいため、計算時間が大きくなってくる。そこで、鍵発行サーバを複数もち、それぞれで鍵発行をすることにより、計算量の分散を図ることがある。

【特許文献1】特開2003-5644号公報

【非特許文献1】岡本龍明、太田和夫共編、「暗号・ゼロ知識問題・数論」、共立出版、1990

【非特許文献2】岡本龍明、山本博資、「現代暗号」、産業図書(1997年)

【非特許文献3】A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, "Handbook of applied cryptography", CRC Press, 1997

【非特許文献4】岡本 栄司、「暗号理論入門」、共立出版、1993、21ページ

【非特許文献5】Henri Cohen, "A Course in Computational Algebraic Number Theory", GTM 138, Springer-Verlag, 1993

【発明の開示】

【発明が解決しようとする課題】

【0015】

鍵発行システムで鍵発行サーバを複数もち場合、鍵発行がシステム全体で正しく行われていることを保証するため、鍵発行システム全体で統一的に同じ鍵発行方法を使用し、管理したいとの要望がある。また、鍵発行サーバでソフトウェアのバグなどにより、正しい鍵発行できない場合がある。システムから与えられた鍵発行方法を用いていることを検証機関により確認できれば、正しく鍵発行していることのある種の根拠となり、統一的な鍵発行を運用するための補助となる。また、鍵発行サーバが不正を働く可能性もあるため、この確認は、鍵発行したサーバ以外が行うのが望ましい。さらに、発行した秘密鍵を用いて確認を行うことは、検証機関が秘密鍵を暴露する可能性があり、望ましくない。したがって、発行した公開鍵を用いて確認できることが望ましい。

【0016】

本発明は、公開鍵を用いて、正しく鍵発行しているかを確認できる鍵発行システムを提供することを目的とする。

【課題を解決するための手段】

【0017】

上記目的を達成するために、請求項1における発明は、鍵発行サーバと、端末装置を備

え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備えることを特徴とする。

【0018】

請求項2における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備えることを特徴とする。

【0019】

請求項3における発明は、前記証明書発行サーバは、さらに、前記公開鍵が前記発行識別子に基づいた前記素数を用いて生成されているかを判定する鍵判定部を備えることを特徴とする。

請求項4における発明は、前記素数生成部は、前記発行識別子情報に基づいて2つの素数を生成することを特徴とする。

【0020】

請求項5における発明は、前記素数生成部は、前記発行識別子情報 $ID I$ 及び $0 \leq c_1$, $c_2 < ID I$ を満たす予め与えられた整数 c_1 , c_2 に対して、 $N_1 = c_1 \bmod ID I$ 及び $N_2 = c_2 \bmod ID I$ を満たす素数 N_1 及び N_2 を生成することを特徴とする。

請求項6における発明は、前記鍵判定部は、前記素数 N_1 及び N_2 の積である前記公開鍵 $n (= N_1 \times N_2)$ と前記整数 c_1 , c_2 に対して、 $n - c_1 \times c_2$ が発行識別子情報 $ID I$ で割り切れることを判定することを特徴とする。

【0021】

請求項7における発明は、前記素数生成部は、第1素数 q 、乱数 R 及び前記発行識別子情報 $ID I$ を用いて $N = 2 \times R \times ID I \times q + 1$ で表される素数 N を生成することを特徴とする。

請求項8における発明は、前記素数生成部は、 len ビットの素数を生成し、 $len q \geq len / 2$ を満たす $len q$ ビットの第1の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 $ID I$ 、前記第1の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times ID I \times q + 1$ なる素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \bmod N$ を満たすか否かを判定する第1の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \bmod N$ を満たすか否かを判定する第2の素数判定部と、を備えることを特徴とする（ここで、 a^x は a の x 乗を示す）。

【0022】

請求項9における発明は、前記素数生成部は、 len ビットの素数を生成し、 $len q \geq len / 2$ を満たす $len q$ ビットの第1の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 $ID I$ 、前記第1の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times ID I \times q + 1$ なる素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \bmod N$ を満たすか否かを判定する第1の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1$

, $N) = 1$ を満たすか否かを判定する第2の素数判定部と、を備えることを特徴とする（ここで、 $GCD(X, Y)$ は X と Y の最大公約数を示す）。

【0023】

請求項10における発明は、前記鍵判定部は、前記公開鍵 n に対して、 $n-1$ が前記発行識別子情報 IDI で割り切れることを判定することを特徴とする。

請求項11における発明は、前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むことを特徴とする。

請求項12における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置であって、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、前記秘密鍵は発行識別子情報に基づいて生成された複数の素数を含むことを特徴とする。

【0024】

請求項13における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置であって、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、前記秘密鍵は発行識別子情報に基づいて生成された複数の素数を含むことを特徴とする。

【0025】

請求項14における発明は、前記秘密鍵は前記発行識別子情報に基づいて生成された2つの素数を含むことを特徴とする。

請求項15における発明は、前記2つの素数は、前記発行識別子情報 IDI 及び $0 \leq c_1$, $c_2 < IDI$ を満たす予め与えられた整数 c_1 , c_2 に対して、 $N_1 = c_1 \bmod IDI$ 及び $N_2 = c_2 \bmod IDI$ を満たす素数 N_1 及び N_2 であることを特徴とする。

【0026】

請求項16における発明は、前記複数の素数は、第1素数 q 、乱数 R 及び前記発行識別子情報 IDI を用いて $N = 2 \times R \times IDI \times q + 1$ で表されることを特徴とする。

請求項17における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備えることを特徴とする。

【0027】

請求項18における発明は、前記素数生成部は、前記発行識別子情報に基づいて2つの素数を生成することを特徴とする。

請求項19における発明は、前記素数生成部は、前記発行識別子情報 IDI 及び $0 \leq c_1$, $c_2 < IDI$ を満たす予め与えられた整数 c_1 , c_2 に対して、 $N_1 = c_1 \bmod IDI$ 及び $N_2 = c_2 \bmod IDI$ を満たす素数 N_1 及び N_2 を生成することを特徴とする。

【0028】

請求項20における発明は、前記素数生成部は、第1素数 q 、乱数 R 及び前記発行識別子情報 IDI を用いて $N = 2 \times R \times IDI \times q + 1$ で表される素数 N を生成することを特徴とする。

請求項21における発明は、前記素数生成部は、 $1 \leq n$ ビットの素数を生成し、 $1 \leq n$, $q \geq 1 \leq n/2$ を満たす $1 \leq n$ ビットの第1の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 IDI 、前記第1の素数 q 及び前

記乱数 R を用いて、 $N = 2 \times R \times IDI \times q + 1$ なる素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \pmod{N}$ を満たすか否かを判定する第 2 の素数判定部と、を備えることを特徴とする。

【0029】

請求項 22 における発明は、前記素数生成部は、 len ビットの素数を生成し、 $len \geq len/2$ を満たす len ビットの第 1 の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 IDI 、前記第 1 の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times IDI \times q + 1$ なる素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第 2 の素数判定部と、を備えることを特徴とする。

【0030】

請求項 23 における発明は、前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むことを特徴とする。

請求項 24 における発明は、素数を生成する素数生成装置であって、前記素数生成装置は、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、を備えることを特徴とする。

【0031】

請求項 25 における発明は、前記素数生成部は、前記発行識別子情報 IDI 及び $0 \leq c < IDI$ を満たす予め与えられた整数 c に対して、 $N = c \pmod{IDI}$ を満たす素数 N を生成することを特徴とする。

請求項 26 における発明は、前記素数生成部は、第 1 素数 q 、乱数 R 及び前記発行識別子情報 IDI を用いて $N = 2 \times R \times IDI \times q + 1$ で表される素数 N を生成することを特徴とする。

【0032】

請求項 27 における発明は、前記素数生成部は、 len ビットの素数を生成し、 $len \geq len/2$ を満たす len ビットの第 1 の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 IDI 、前記第 1 の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times IDI \times q + 1$ なる素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $2^{(2R)} \neq 1 \pmod{N}$ を満たすか否かを判定する第 2 の素数判定部と、を備えることを特徴とする。

【0033】

請求項 28 における発明は、前記素数生成部は、 len ビットの素数を生成し、 $len \geq len/2$ を満たす len ビットの第 1 の素数 q を生成する素数情報生成手段と、乱数 R を生成する乱数生成手段と、前記発行識別子情報 IDI 、前記第 1 の素数 q 及び前記乱数 R を用いて、 $N = 2 \times R \times IDI \times q + 1$ なる素数候補 N を生成する素数候補生成部と、前記素数候補 N に対し、 $2^{(N-1)} = 1 \pmod{N}$ を満たすか否かを判定する第 1 の素数判定部と、前記素数候補 N 及び前記乱数 R に対し、 $GCD(2^{(2R)} - 1, N) = 1$ を満たすか否かを判定する第 2 の素数判定部と、を備えることを特徴とする。

【0034】

請求項 29 における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから RSA 暗号の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行方法であって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を

備えることを特徴とする。

【0035】

請求項30における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行方法であって、前記鍵発行サーバは、データを送信する送信部と、データを受信する受信部と、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備えることを特徴とする。

【0036】

請求項31における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、前記プログラムは、素数を含む前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵を格納する公開鍵格納ステップと、を前記端末装置に実行させ、前記秘密鍵は発行識別子情報に基づいて生成された素数を含むことを特徴とする。

【0037】

請求項32における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、前記プログラムは、前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵証明書を格納する公開鍵証明書格納ステップと、を前記端末装置に実行させ、前記秘密鍵は発行識別子情報に基づいて生成された素数を含むことを特徴とする。

【0038】

請求項33における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバに実行させるプログラムであって、前記プログラムは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成ステップと、を前記鍵発行サーバに実行させることを特徴とする。

【0039】

請求項34における発明は、素数を生成する素数生成装置に実行させるプログラムであって、前記プログラムは、発行識別子を生成する発行識別子生成ステップと、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、を前記素数生成装置に実行させることを特徴とする。

請求項35における発明は、請求項31から請求項34のいずれか1項に記載のプログラムを記録した媒体である。

【発明の効果】

【0040】

これらの構成によると、正しく鍵発行しているかを発行識別子情報 ID I で割り切れるかをチェックすることで確認でき、その価値は大きい。

【発明を実施するための最良の形態】

【0041】

(実施の形態1)

本発明に係る 1 の実施の形態としての素数生成装置 1 について、説明する。

図 1 は、実施の形態 1 における素数生成装置の構成を示す図である。

この素数生成装置 1 は、素数 q 、 q のビットサイズ $\text{len } q$ 、発行識別子情報 IDI 及び識別子のビットサイズ len IDI が与えられたとき、 q のビットサイズ $\text{len } q$ の 2 倍のビットサイズ $2 \times \text{len } q$ をもつ素数を出力するものである。

【0042】

<素数生成装置 1 の構成>

素数生成装置 1 は、乱数生成部 11 と、素数候補生成部 12 と、第 1 素数判定部 13 と、第 2 素数判定部 14 と、を備える。

乱数生成部 11 は、 $\text{len } q$ を用いて、 $(\text{len } q - \text{len IDI} - 1)$ ビットの乱数 R' を生成する。ここで、乱数 R' の最上位ビットは 1 とする。

【0043】

素数候補生成部 12 は、 q 及び R' を用いて、以下の式を満たす R と N を生成する。

$$\begin{aligned} R &= \text{IDI} \times R' \\ N &= 2 \times R \times q + 1 \end{aligned}$$

第 1 素数判定部 13 は、 N を用いて、以下の式の成立を判定する。

【0044】

$$2^{(N-1)} = 1 \pmod{N} \quad (\text{eq 1})$$

ここで、 $2^{(N-1)}$ は、2 の $N-1$ 乗を示している。

第 2 素数判定部 14 は、 N と R を用いて、以下の式を満たすか否かを判定する。

$$2^{(2R)} \neq 1 \pmod{N} \quad (\text{eq 2})$$

<素数生成装置 1 の動作>

以下に素数生成装置 1 の動作を示す。図 2 にこの動作のフローチャートを示す。

【0045】

ステップ S101: 乱数生成部 11 は、 $(\text{len } q - \text{len IDI} - 1)$ ビットの乱数 R' を生成する。ここで、 R' の最上位ビットは 1 とする。

ステップ S102: 素数候補生成部 12 は、 R と N を計算する。

ステップ S103: 第 1 素数判定部 13 は、 $2^{(N-1)} = 1 \pmod{N}$ の成立を判定する。この式が成立する場合は次の S104 ステップへ。成立しない場合はステップ S101 へ。

【0046】

ステップ S104: 第 2 素数判定部 14 は、 $2^{(2R)} \neq 1 \pmod{N}$ を満たすか否かを判定する。この式が成立する場合は N を出力し、終了する。成立しない場合は、ステップ S101 へ。

<実施の形態 1 の効果>

生成された素数 N に対して、 $N-1$ は必ず発行識別子情報 IDI で割り切れる。なぜなら、 $N-1 = 2 \times q \times R = 2 \times q \times \text{IDI} \times R'$ が成り立つためである。したがって、生成された素数が発行識別子情報 IDI で割り切れるか否かで、素数生成装置 1 を用いて素数が生成されたかを確認することができる。

【0047】

なお、 IDI のビットサイズが len IDI であり、 R' のビットサイズが $(\text{len } q - \text{len IDI} - 1)$ であるため、ほとんどの $N = 2 \times q \times \text{IDI} \times R' + 1$ のビットサイズは、 $2 \times \text{len } q$ となる。ここで、 q や IDI などの値によっては、ビットサイズが $2 \times \text{len } q - 1$ となる場合がある。その場合は、素数候補生成部 12 で、 R' に 2 を掛けて、それを新たに R' とみなすことにより、 N のビットサイズを $2 \times \text{len } q$ になるように設定する。

【0048】

(実施の形態 2)

本発明に係る 2 の実施の形態としての素数生成装置 2 について、説明する。

図 3 は、実施の形態 2 における素数生成装置の構成を示す図である。

この素数生成装置 2 は、素数 q 、 q のビットサイズ $\text{len } q$ 、発行識別子情報 IDI 、発行識別子情報のビットサイズ len IDI 及び検証値 c が与えられたとき、 q のビットサイズ $\text{len } q$ の 2 倍のビットサイズ $2 \times \text{len } q$ をもつ素数を出力するものである。ここで、 IDI は奇数とする。

【0049】

＜素数生成装置 2 の構成＞

素数生成装置 2 は、実施形態 1 の素数生成装置 1 と同様の乱数生成部 11 と、第 1 素数判定部 13 と、第 2 素数判定部 14 と、素数生成装置 2 と異なる素数候補生成部 22 と、を備える。

素数候補生成部 22 は、 q 及び R' を用いて、以下の式を満たす R と N を生成する。

【0050】

$$R = \text{IDI} \times R'$$

$$N = 2 \times (R + w) \times q + 1$$

ここで、 w は $2 \times w \times q + 1 = c \pmod{\text{IDI}}$ 、 $0 \leq w < \text{IDI}$ を満たす数である。 w は、 $w = (c - 1) \times m \pmod{\text{IDI}}$ を計算することにより求める。 m は $(2 \times q) \times m = 1 \pmod{\text{IDI}}$ を満たす数である。 IDI が奇数、すなわち、 $\text{GCD}(\text{IDI}, 2) = 1$ であり、 $\text{IDI} < q$ であるため、 m は計算可能である。計算方法については、非特許文献 5 が詳しい。

【0051】

＜素数生成装置 2 の動作＞

以下に素数生成装置 2 の動作を示す。図 4 にこの動作のフローチャートを示す。

ステップ S201：乱数生成部 11 は、 $(\text{len } q - \text{len IDI} - 1)$ ビットの乱数 R' を生成する。ここで、 R' の最上位ビットは 1 とする。

【0052】

ステップ S202：素数候補生成部 22 は、 R と N を計算する。

ステップ S203：第 1 素数判定部 13 は、 $2^{(N-1)} = 1 \pmod{N}$ の成立を判定する。この式が成立する場合は次のステップ S204 へ。成立しない場合はステップ S201 へ。

ステップ S204：第 2 素数判定部 14 は、 $2^{(2R)} \neq 1 \pmod{N}$ の成立を判定する。この式が成立する場合は N を出力し、終了する。成立しない場合は、ステップ S201 へ。

【0053】

＜実施の形態 2 の効果＞

生成された素数 N に対して、 $N - c$ は必ず発行識別子情報 IDI で割り切れる。なぜなら、 $N - c = 2 \times q \times R + 1 - c = 2 \times q \times (\text{IDI} \times R' + w) + 1 - c$ であり、 $2 \times q \times w + 1 = c \pmod{\text{IDI}}$ が成り立つためである。したがって、生成された素数 N に対し、 $N - c$ が発行識別子情報 IDI で割り切れるか否かで、素数生成装置 2 を用いて素数が生成されたかを確認することができる。

【0054】

なお、 IDI のビットサイズが len IDI であり、 R' のビットサイズが $(\text{len } q - \text{len IDI} - 1)$ であるため、ほとんどの $N = 2 \times q \times (\text{IDI} \times R' + w) + 1$ のビットサイズは、 $2 \times \text{len } q$ となる。ここで、 q や IDI などの値によっては、ビットサイズが $2 \times \text{len } q - 1$ となる場合がある。その場合は、素数候補生成部 12 で、 R' に 2 を掛けて、それを新たに R' とみなすことにより、 N のビットサイズを $2 \times \text{len } q$ になるように設定する。

【0055】

（実施の形態 3）

本発明に係る 3 の実施の形態としての鍵発行システム 3 について、説明する。

図 5 は、実施の形態 3 における鍵発行システム 3 の構成を示す図である。本システムは、鍵発行サーバ A31、B32、C33 と、証明書発行サーバ 34 と、端末装置 351、3

52、353、...、35 n から構成される。 n は自然数であり、例えば1000である。この場合、端末装置が1000台存在することになる。

＜鍵発行サーバA31、B32、C33の構成＞

鍵発行サーバA31、B32、C33は同じ構成であるため、以下では代表して鍵発行サーバA31の構成を示す。鍵発行サーバA31、B32、C33にはそれぞれ、予め識別子：SIDA、SIDB、SIDCが与えられている。

【0056】

鍵発行サーバA31は、予め与えられた検証値 c_1 、 c_2 を用いてRSA暗号における秘密鍵及び公開鍵を生成し、公開鍵を証明書発行サーバへ送信し、公開鍵証明書を受信した後、端末装置へ送信する。

鍵発行サーバA31は、送信部3101と、受信部3102と、識別子生成部3103、識別子格納部3104と、素数生成部3105と、秘密鍵判定部3106と、鍵生成部3107と、秘密鍵格納部3108と、公開鍵格納部3109と、証明書格納部3110を備える（図6参照）。

【0057】

送信部3101は、端末装置35 i （ $i=1\sim n$ ）へ生成した秘密鍵及び公開鍵を、証明書発行サーバ34へ公開鍵を送信する。

受信部3102は、端末装置35 i から鍵生成要求情報を、証明書発行サーバ34から公開鍵証明書Certを受信する。公開鍵証明書については、証明書発行サーバ34の構成の説明で述べる。

【0058】

識別子生成部3103は、端末装置35 i 用に素数の発行識別子情報IDIを生成し、識別子格納部3104に格納する。発行識別子情報IDIは、予め与えられた各鍵発行サーバに対応する識別子：SID（A31はSIDA、B32はSIDB、C33はSIDC）と発行識別子：PIDからなる。例えば、 $IDI = SID || PID$ とする。ここで、 $||$ はビットまたはバイト連結である。発行識別子は例えば、1から発行順に数字を割り当て、発行するたびにインクリメントする。

【0059】

識別子格納部3104は、素数の発行識別子情報IDIを格納する。

素数生成部3105は、512ビット素数を生成する。なお、ここでは鍵長が1024ビットのRSAを想定しているため、512ビット素数を生成するとしたが、鍵長を len ビットとして、 $len/2$ ビットの素数を生成するとしてもよい。

（素数生成部3105の構成及び動作）

素数生成部3105は、第1の素数生成部31051と、第2の素数生成部31052と、を備える（図7参照）。

【0060】

第1の素数生成部31051は、256ビットの素数 q を生成する。素数の生成方法は従来の方法を用いる。従来の方法については、特許文献1及び非特許文献3が詳しい。

第2の素数生成部31052は、256ビット素数 q と、 q のビットサイズ256と、発行識別子情報IDI及び、予め与えられた検証値 c_1 または c_2 を用いて、512ビットの素数 N を生成する。第2の素数生成部31052は、実施形態2の素数生成装置2を用いて、素数 N を生成する。

【0061】

秘密鍵判定部3106は、2回の素数生成部3105の処理を実行して出力された素数 p_1 と p_2 が一致しているかを比較する。

鍵生成部3107は、秘密鍵格納部3108に格納されている秘密鍵 p_1 、 p_2 の積 $n = p_1 \times p_2$ を計算し、さらに、乱数 e を生成し、それらの n と e の組 $PK = (n, e)$ を公開鍵とする。

【0062】

その後、 $e \times d = 1 \pmod{L}$ を満たす d を計算し秘密鍵とする。ここで、 $L = \text{LCM}(p_1 - 1, p_2 - 1)$ である。 $\text{LCM}(p_1 - 1, p_2 - 1)$ は $p_1 - 1$ と $p_2 - 1$ の最小公倍数を示す。

秘密鍵格納部3108は、素数生成部3105で生成した2つの素数 p_1 、 p_2 と鍵生成部で作成した d の組 $SK = (p_1, p_2, d)$ を秘密鍵として格納する。

【0063】

公開鍵格納部3109は、鍵生成部3107で生成した公開鍵 PK を格納する。

証明書格納部3110は、証明書発行サーバ34が送信した公開鍵証明書 $Cert$ を格納する。

<鍵発行サーバA31、B32、C33の動作>

鍵発行サーバA31、B32、C33の動作は同様であるため、以下に代表して鍵発行サーバA31の動作を示す。ここでは、端末装置35i (i は1から n のいずれかの数)から鍵発行依頼情報が送信された場合の動作を示している。図8にこの動作のフローチャートを示す。

【0064】

ステップS301: 受信部312は、端末装置35iより送信された鍵発行依頼情報を受信する。

ステップS302: 識別子生成部313は、発行識別子情報: IDI を生成し、識別子格納部214に格納する。

ステップS303: 素数生成部315は、予め与えられた検証値 c_1 を用いて、素数 p_1 を生成する。

【0065】

ステップS304: 素数生成部315は、予め与えられた検証値 c_2 を用いて、素数 p_2 を生成する。

ステップS305: 秘密鍵判定部316は、素数 p_1 と p_2 が $p_1 = p_2$ を満たすかを判定する。 $p_1 = p_2$ の場合は、ステップS304へ。それ以外は、秘密鍵格納部318に格納する。次のステップS306へ。

【0066】

ステップS306: 鍵生成部317は、 $n = p_1 \times p_2$ を計算する。また、鍵生成部317は、乱数 e を生成し、 n と e の組 $PK = (n, e)$ を公開鍵として公開鍵格納部319に格納する。さらに、鍵生成部317は、 $e \times d = 1 \pmod{L}$ を満たす d を計算し、 p_1 、 p_2 と d の組 $SK = (p_1, p_2, d)$ を秘密鍵として秘密鍵格納部318に格納する。

【0067】

ステップS307: 送信部311は、公開鍵格納部319に格納されている公開鍵 PK 及び識別子格納部314に格納されている発行識別子情報 IDI を証明書発行サーバ34へ送信する。

ステップS308: 受信部312は、証明書発行サーバ34より送信された公開鍵証明書 $Cert$ を受信する。

【0068】

ステップS309: 送信部311は、秘密鍵格納部318に格納されている秘密鍵 $SK = (p_1, p_2, d)$ と、公開鍵証明書 $Cert$ を端末装置35iへ送信し、終了する。

<証明書発行サーバ34の構成>

証明書発行サーバ34は、送信部341と、受信部342と、秘密鍵格納部343と、発行公開鍵確認部344と、発行公開鍵格納部345と、発行識別子情報格納部346と、公開鍵証明書生成部347と、公開鍵証明書格納部348と、を備える(図9参照)。

【0069】

送信部341は、証明書 $Cert$ を鍵発行サーバA31、B32または、C33へ送信する。

受信部342は、鍵発行サーバA31、B32または、C33から公開鍵 n 、 e を受信

する。

秘密鍵格納部 343 は、証明書発行サーバ 34 の秘密鍵 SKCA を格納する。

【0070】

発行公開鍵確認部 344 は、鍵発行サーバ A 31、B 32 または C 33 から受信した公開鍵 PK = (n, e) と発行識別子情報 IDI を用いて、公開鍵 PK = (n, e) が発行識別子情報 IDI を用いて生成されたかを確認する。具体的には、検証値 c1 及び c2 を用いて、 $n - c1 \times c2$ が IDI で割り切れるかでチェックする。割り切れる場合は、公開鍵 PK = (n, e) が発行識別子情報 IDI で生成されたと判断し、それ以外は発行識別子情報 IDI で生成されていないと判断する。

【0071】

発行公開鍵格納部 345 は、鍵発行サーバ A 31、B 32 または C 33 から受信した公開鍵 PK = (n, e) を格納する。

発行識別子情報格納部 346 は、鍵発行サーバ A 31、B 32 または C 33 から受信した発行識別子情報 IDI を格納する。

公開鍵証明書生成部 347 は、公開鍵 PK と発行識別子情報 IDI に対する公開鍵証明書 Cert を、秘密鍵格納部 343 に格納されている秘密鍵 SKCA を用いて生成する。具体的には、例えば、 $Cert = n || e || IDI || Sig(SKCA, n || e || IDI)$ とする。ここで、 $Sig(K, D)$ はデータ D に対する鍵 K を用いたときの署名データである。また、 $||$ はビットまたはバイトの連結である。

【0072】

公開鍵証明書格納部 348 は、公開鍵証明書 Cert を格納する。

<証明書発行サーバ 34 の動作>

以下に証明書発行サーバ 34 の動作を示す。ここでは、証明書を発行する先を鍵発行サーバ A 31 として動作を示す。なお、他の鍵発行サーバ (B 32、C 33) を発行先の場合も同様の動作を行う。図 10 にこの動作のフローチャートを示す。

【0073】

ステップ S401: 受信部 342 は、鍵発行サーバ A 31 から送信された公開鍵 PK = (n, e) と発行識別子情報 IDI を受信する。

ステップ S402: 発行公開鍵確認部 344 は、公開鍵 PK = (n, e) が発行識別子情報 IDI を用いて生成されたかを確認する。公開鍵 PK = (n, e) が発行識別子情報 IDI で生成されていると判断した場合は、次のステップ S403 へ。それ以外は、システムを終了する。

【0074】

ステップ S403: 発行公開鍵格納部 345 は、公開鍵 PK = (n, e) を、発行識別子情報格納部 346 は、発行識別子情報 IDI をそれぞれ格納する。

ステップ S404: 公開鍵証明書生成部 347 は、公開鍵 PK = (n, e) と発行識別子情報 IDI に対する公開鍵証明書 Cert を生成し、公開鍵証明書格納部 348 に格納する。

【0075】

ステップ S405: 送信部 341 は、公開鍵証明書格納部 348 に格納されている公開鍵証明書 Cert を鍵発行サーバ A 31 へ送信し、終了する。

<端末装置 35i (i = 1 ~ n) の構成>

端末装置 351、352、353、...、35n はそれぞれ、同じ構成をしているため、以下では代表して、端末装置 35i の構成を示す。

【0076】

端末装置 35i は、送信部 35i1 と、受信部 35i2 と、秘密鍵格納部 35i3 と、公開鍵格納部 35i4 と、発行識別子情報格納部 35i5 と、を備える (図 11 参照)。

送信部 35i1 は、鍵発行依頼情報を鍵発行サーバ A 31、B 32、C 33 のいずれかへ送信する。鍵発行依頼情報は、例えば、端末装置 35i を示す識別子情報などである。

受信部 35i2 は、鍵発行サーバ A 31、B 32、C 33 のいずれかから送信された秘

密鍵 $SK = (p1, p2, d)$ 、公開鍵 $PK = (n, e)$ と、発行識別子情報 IDI を受信する。

【0077】

秘密鍵格納部 35i3 は、秘密鍵 $SK = (p1, p2, d)$ を格納する。

公開鍵証明書格納部 35i4 は、公開鍵証明書 $Cert$ を格納する。

<端末装置 35i の動作>

以下に端末装置 35i の動作を示す。ここでは、鍵発行サーバ A31 に鍵発行を依頼する場合の動作を示している。図 12 にこの動作のフローチャートを示す。

【0078】

ステップ S501: 送信部 35i1 は、鍵発行依頼情報を鍵発行サーバ A31 へ送信する。

ステップ S502: 受信部 35i2 は、鍵発行サーバ A31 より送信された秘密鍵 $SK = (p1, p2, d)$ 、公開鍵証明書 $Cert$ を受信する。

ステップ S503: 秘密鍵格納部 35i3 は、秘密鍵 $SK = (p1, p2, d)$ を格納する。

【0079】

ステップ S504: 公開鍵証明書格納部 35i4 は、公開鍵証明書 $Cert$ を格納し、終了する。

<鍵発行システム 3 の動作>

以下に鍵発行システム 3 の動作を示す。以下では、鍵発行サーバ A31 が端末装置 35i に鍵を発行するときの動作を示す。端末装置 35i は、まず、鍵発行依頼情報を鍵発行サーバ A31 へ送信する。鍵発行サーバ A31 は、鍵発行依頼情報を受信した後、発行識別子情報 IDI を作成する。その後、鍵発行サーバ A31 は秘密鍵 $SK = (p1, p2, d)$ 、公開鍵証明書 $PK = (n, e)$ を生成する。さらに、鍵発行サーバ A31 は、公開鍵 $PK = (n, e)$ と発行識別子情報 IDI を証明書発行サーバ 34 へ送信する。証明書発行サーバ 34 は、公開鍵 PK に対応する秘密鍵 SK に含まれる素数 $p1$ 、 $p2$ が発行識別子情報 IDI を用いて生成されているかを判定する。証明書発行サーバ 34 は、判定結果が肯定的な場合に、公開鍵 PK に対する公開鍵証明書 $Cert$ を生成し、公開鍵証明書 $Cert$ を鍵発行サーバ A31 へ送信する。鍵発行サーバ A31 は、秘密鍵 $SK = (p1, p2, d)$ と公開鍵証明書 $Cert$ を端末装置 35i へ送信する。端末装置 35i は、秘密鍵 SK 、公開鍵証明書 $Cert$ を格納し、システムを終了する。

【0080】

<実施の形態 3 の効果>

証明書発行サーバは、鍵発行サーバが正しく発行識別子情報 IDI を用いて生成しているかを確認することができる。なぜなら、秘密鍵である素数 $p1$ 、 $p2$ はそれぞれ、素数 $q1$ 、 $q2$ 、乱数 $R1'$ 、 $R2'$ 、発行識別子情報 IDI に対して、 $p1 = 2 \times q1 \times (IDI \times R1' + r1') + 1 = c1 \mod IDI$ 、 $p2 = 2 \times q2 \times (IDI \times R2' + r2') + 1 = c2 \mod IDI$ を満たすため、

$$n = p1 \times p2 = (2 \times q1 \times IDI \times R1' + 1) \times (2 \times q2 \times IDI \times R2' + 1)$$

$$= c1 \times c2 \mod IDI$$

となる。そのため、 $n - c1 \times c2$ は IDI で割り切れるため、 $n - c1 \times c2$ が IDI で割り切れることを確認することで、素数 $p1$ 、 $p2$ が正しく発行識別子情報 IDI を用いて生成しているかを確認することができる。

【0081】

なお、端末がその端末がもつ秘密鍵を用いて、不正を働いたとき、以下の確認方法により、秘密鍵より不正を働いた端末の情報を得ることができる。不正を働いた端末の秘密鍵 $p1$ 、 $p2$ が判明したとする。また、不正の追跡者は、発行識別子情報と端末の対応表と持っているとする。 $p1 - c1$ 、 $p2 - c2$ は共に発行識別子情報 IDI で割り切れる。そのため、 $GCD(p1 - c1, p2 - c2)$ は発行識別子情報で割り切れる。したがっ

て、 $GCD(p_1 - c_1, p_2 - c_2)$ の素因数を調べることにより、不正の追跡者は、取りうる発行識別子情報を限定でき、発行識別子情報を知る、すなわち、端末を特定するための助けとなる。

【0082】

(変形例)

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。例えば、以下のような場合も本発明に含まれる。

(1) 先にも述べたが、実施の形態3における、生成する秘密鍵である素数のビットサイズは512に限らない。1024であっても、2048であってもよい。また、素数情報生成部で生成する素数も同様に256ビットに限らない。

【0083】

(2) 実施の形態3の鍵発行サーバは、素数生成装置2を使用しているが、素数生成装置1を使用してもよい。その場合は、証明書発行サーバは $n-1$ がIDIで割り切れることを確認する。

(3) 実施の形態1、または2の素数生成装置を素数生成手段として用いて、整数 len と発行識別子情報IDIを入力とし、 len ビットの素数を出力する素数生成装置としてもよい。

【0084】

(4) 鍵発行サーバは3台以外の何台であってもよい。

【産業上の利用可能性】**【0085】**

これらの構成によると、正しく鍵発行しているかを発行識別子情報IDIで割り切れるかをチェックすることで確認できる。

【図面の簡単な説明】**【0086】**

【図1】 本発明に係る1個の実施の形態としての素数生成装置1の構成を示すブロック図

【図2】 素数生成装置1の動作を示すフローチャート

【図3】 本発明に係る1個の実施の形態としての素数生成装置2の構成を示すブロック図

【図4】 素数生成装置2の動作を示すフローチャート

【図5】 本発明に係る1個の実施の形態としての鍵発行システム3の構成を示すブロック図

【図6】 鍵発行サーバA31の構成を示す図

【図7】 素数生成部3105の構成を示す図

【図8】 鍵発行サーバA31の動作を示すフローチャート

【図9】 証明書発行サーバ34の構成を示す図

【図10】 証明書発行サーバ34の動作を示すフローチャート

【図11】 端末装置35iの構成を示す図

【図12】 端末装置35iの動作を示すフローチャート

【符号の説明】**【0087】**

1、2 素数生成装置

11 乱数生成部

12、22 素数候補生成部

13 第1素数判定部

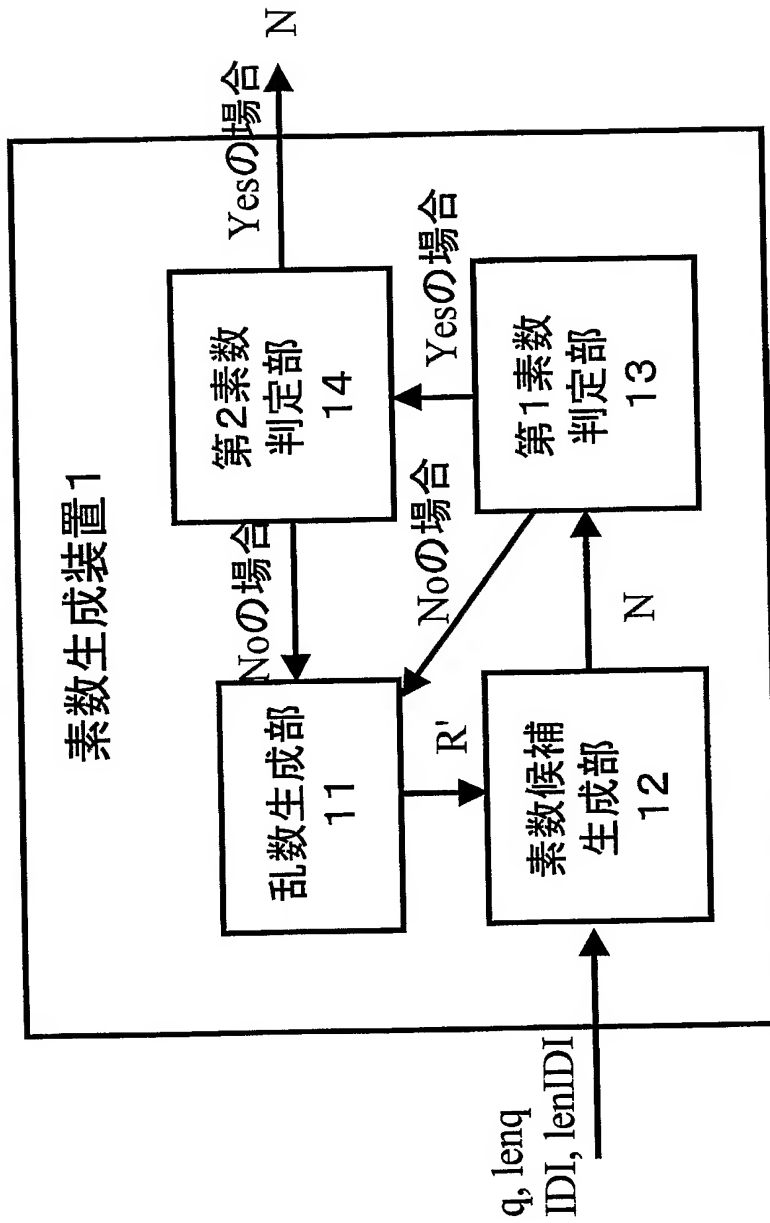
14 第2素数判定部

3 鍵発行システム

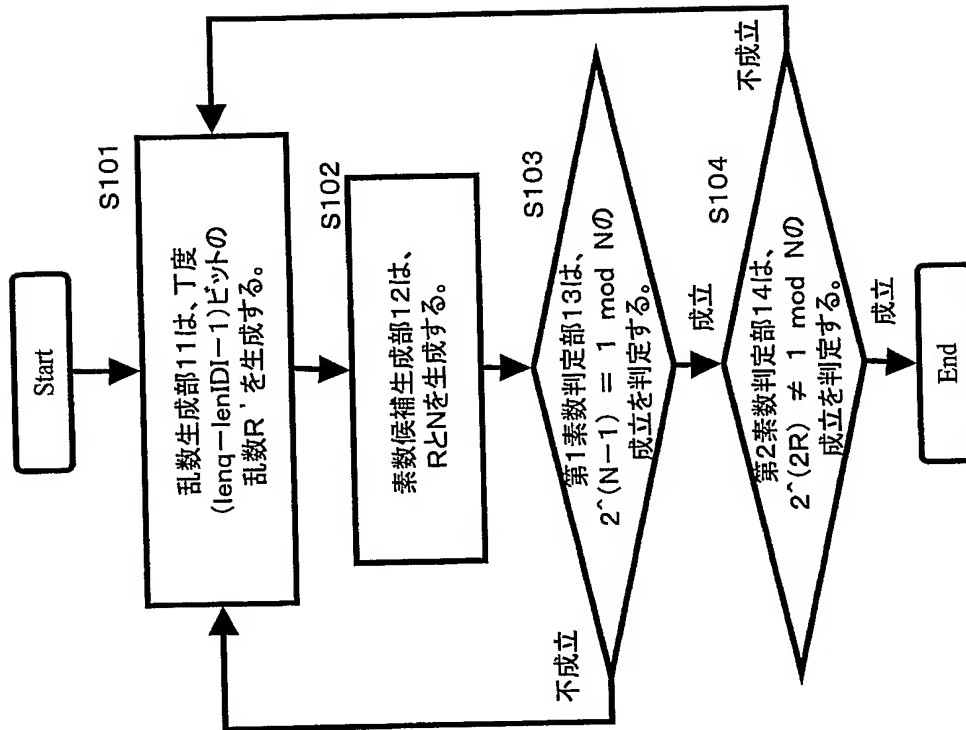
31 鍵発行サーバA

3 1 0 1、3 4 1、3 5 i 1 送信部
3 1 0 2、3 4 2、3 5 i 2 受信部
3 1 0 3 識別子生成部
3 1 0 4 識別子格納部
3 1 0 5 素数生成部
3 1 0 5 1 第 1 の素数生成部
3 1 0 5 2 第 2 の素数生成部
3 1 0 6 秘密鍵判定部
3 1 0 7 鍵生成部
3 1 0 8、3 4 3、3 5 i 3 秘密鍵格納部
3 1 0 9 公開鍵格納部
3 1 1 0、3 4 7、3 5 i 4 公開鍵証明書格納部
3 2 鍵発行サーバ B
3 3 鍵発行サーバ C
3 4 証明書発行サーバ
3 4 4 発行公開鍵確認部
3 4 5 発行公開鍵格納部
3 4 6 公開鍵証明書生成部
3 5 i (i = 1 ~ n) 端末装置

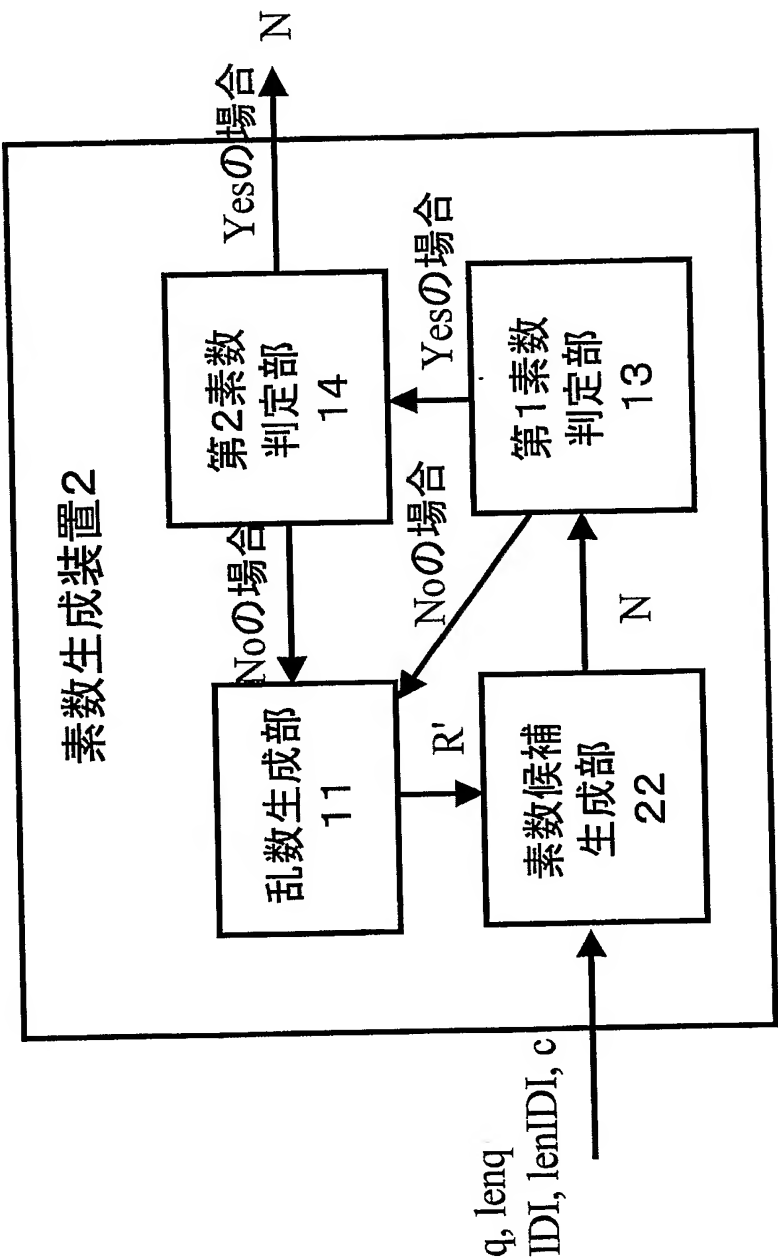
【書類名】 図面
【図 1】



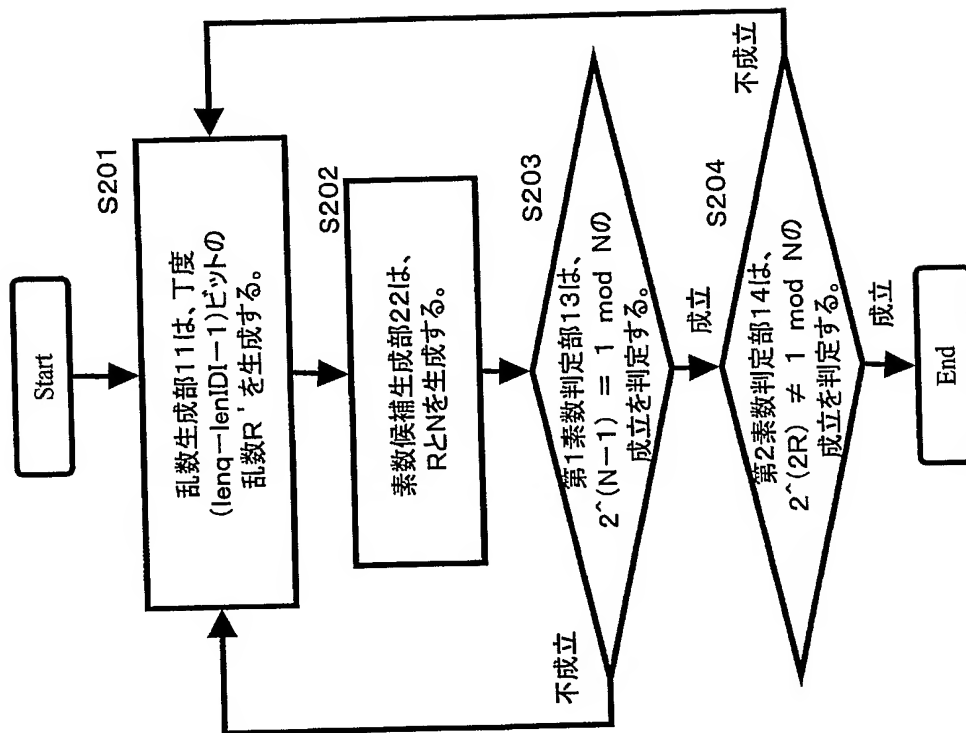
【図 2】



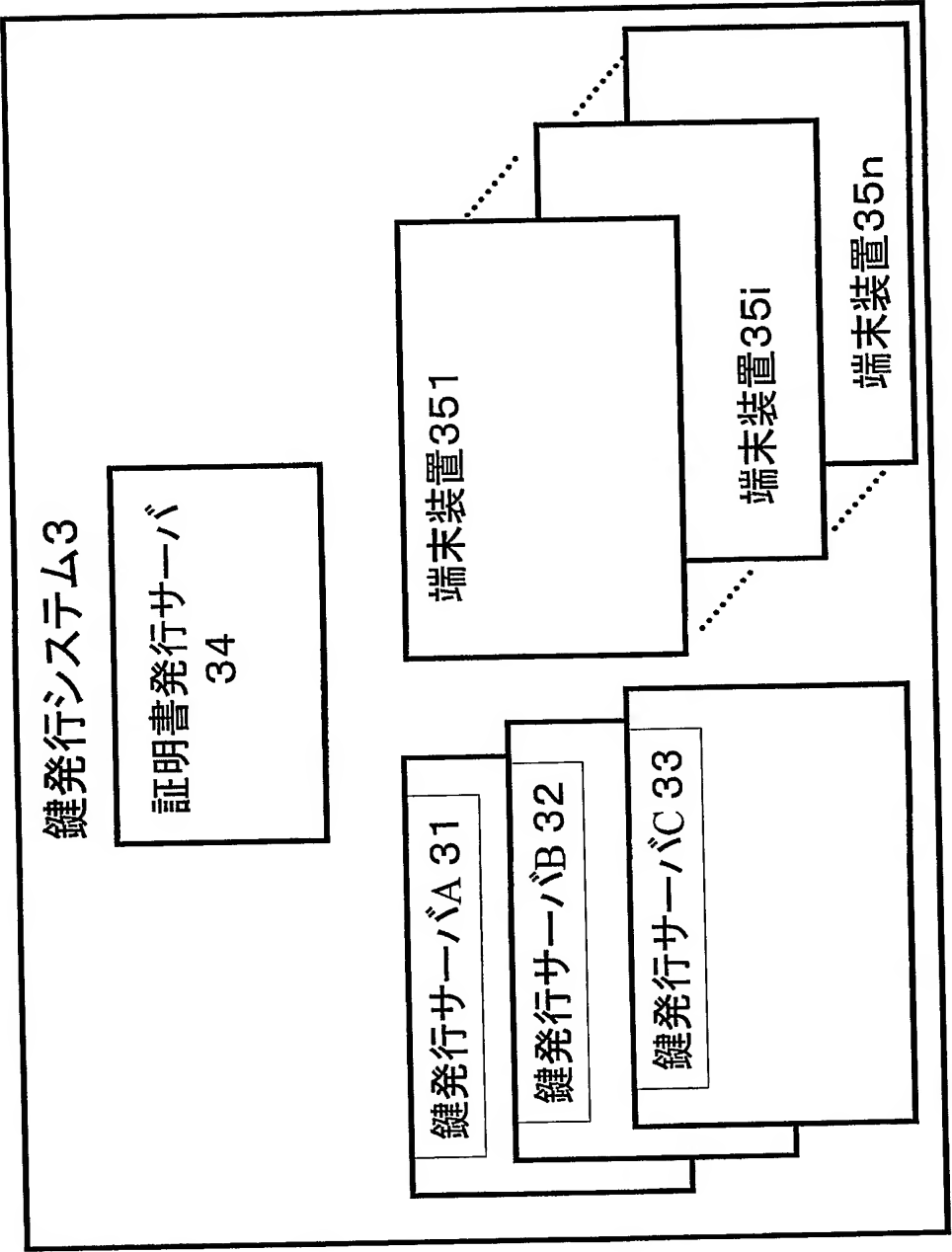
【図 3】



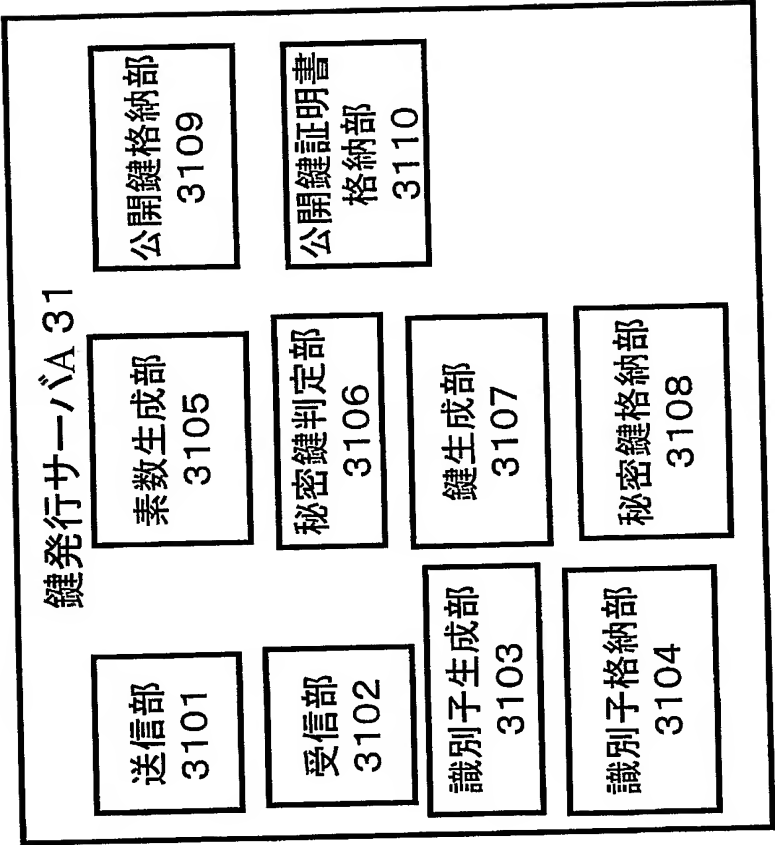
【図 4】



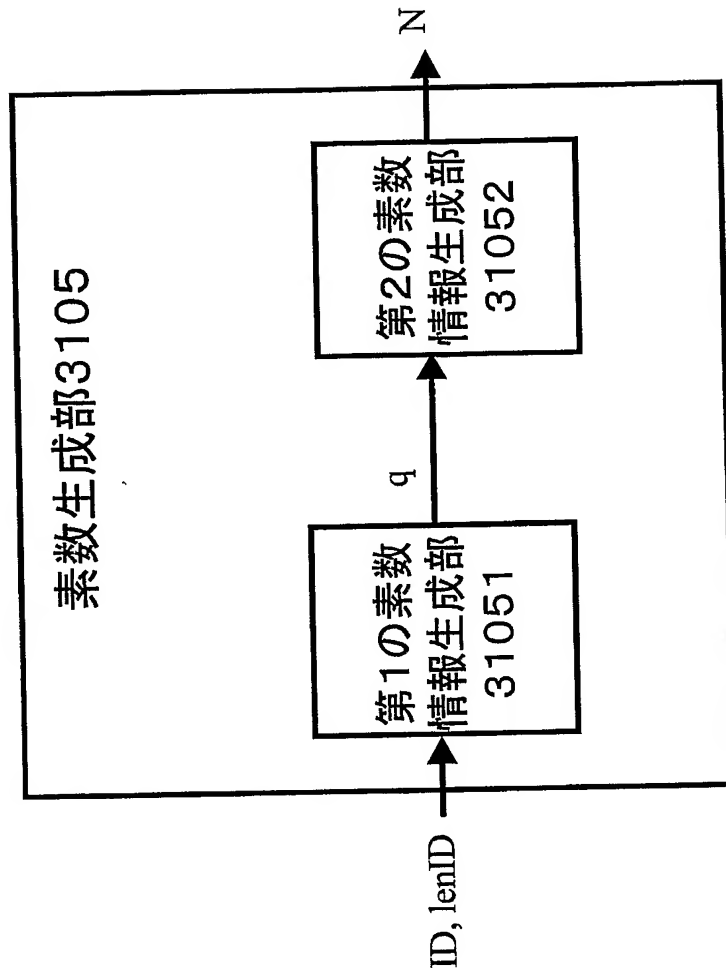
【図 5】



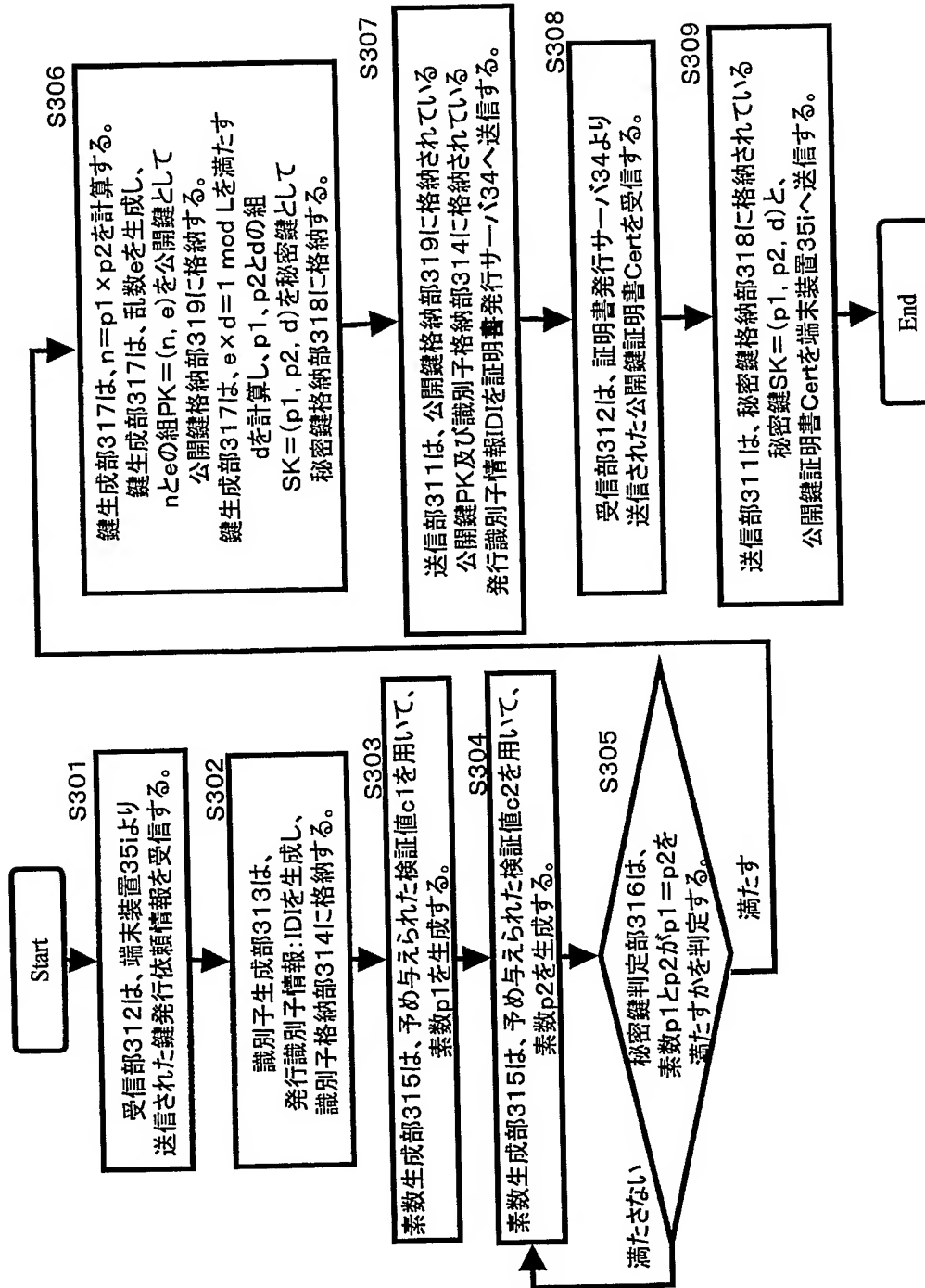
【図 6】



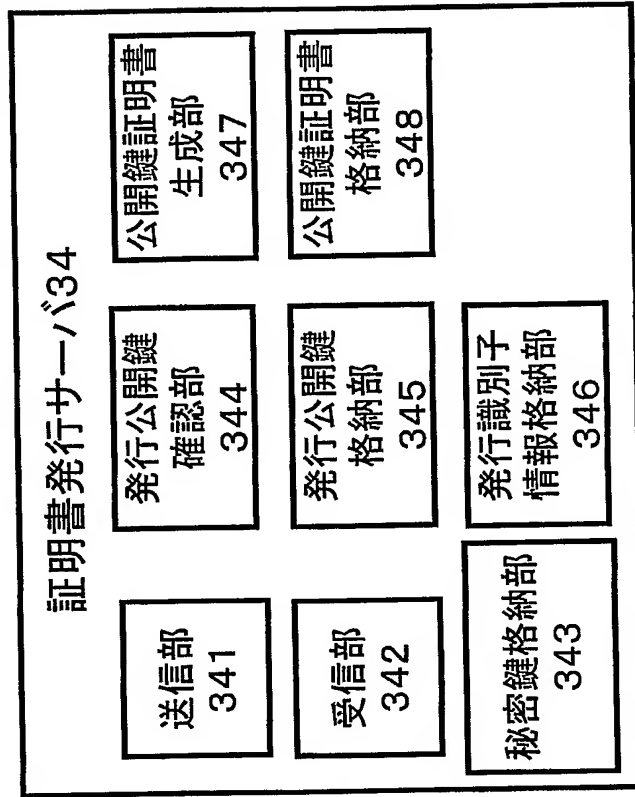
【図 7】



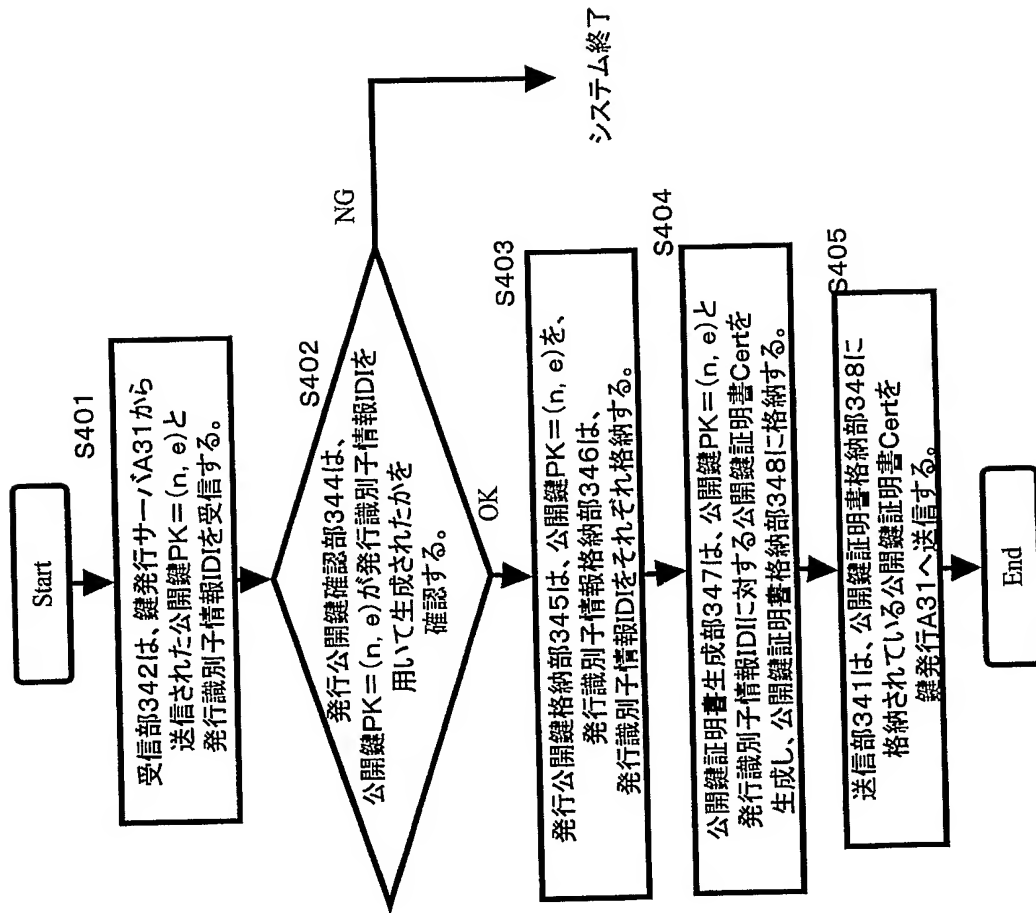
【図 8】



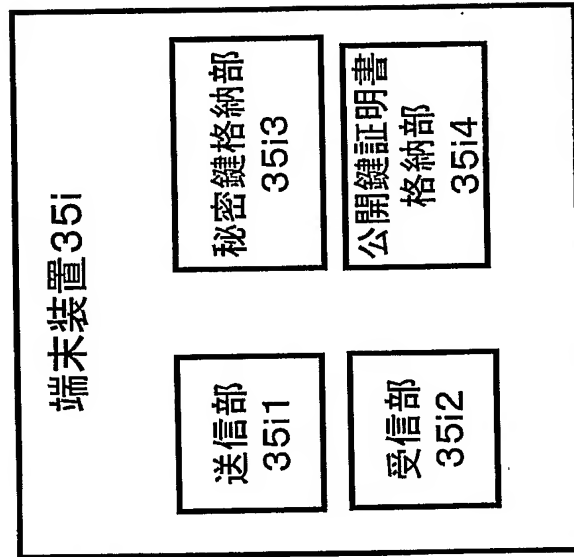
【図 9】



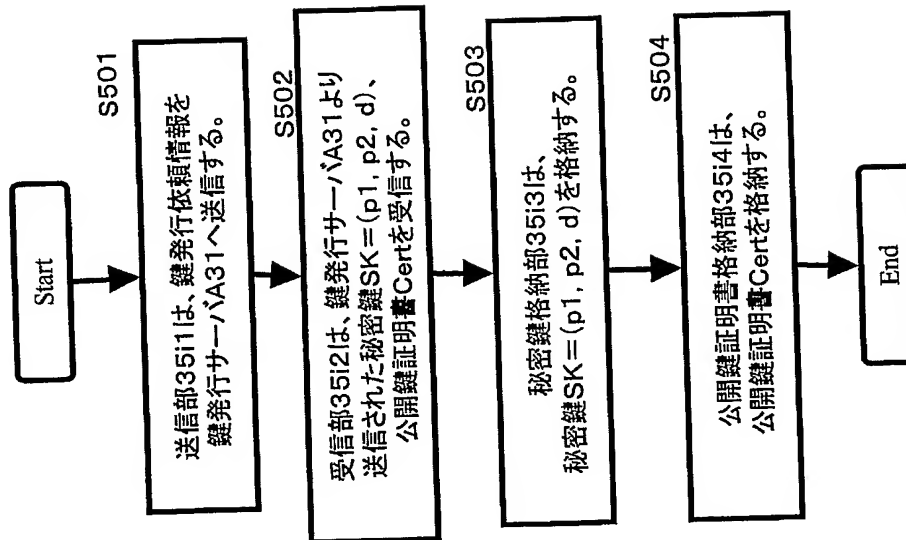
【図 10】



【図 1 1】



【図 12】



【書類名】要約書**【要約】**

【課題】 鍵発行システムで鍵発行サーバを複数もつ場合、鍵発行がシステム全体で正しく行われていることを保証するため、鍵発行システム全体で統一的に同じ鍵発行方法を使用し、管理したいとの要望がある。そこで、鍵発行システムで、鍵発行サーバが正しく鍵発行しているかを判定する方法があればよい。

【解決手段】 鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備えることにより、素数に発行識別子を埋め込み、発行識別子埋め込みを、公開鍵を用いて確認する。

【選択図】 図 5

特願 2 0 0 3 - 4 3 3 9 0 4

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社